


Using PCP (RFC6887) with CoAP endpoints

Jaime Jiménez
jaime.jimenez@ericsson.com

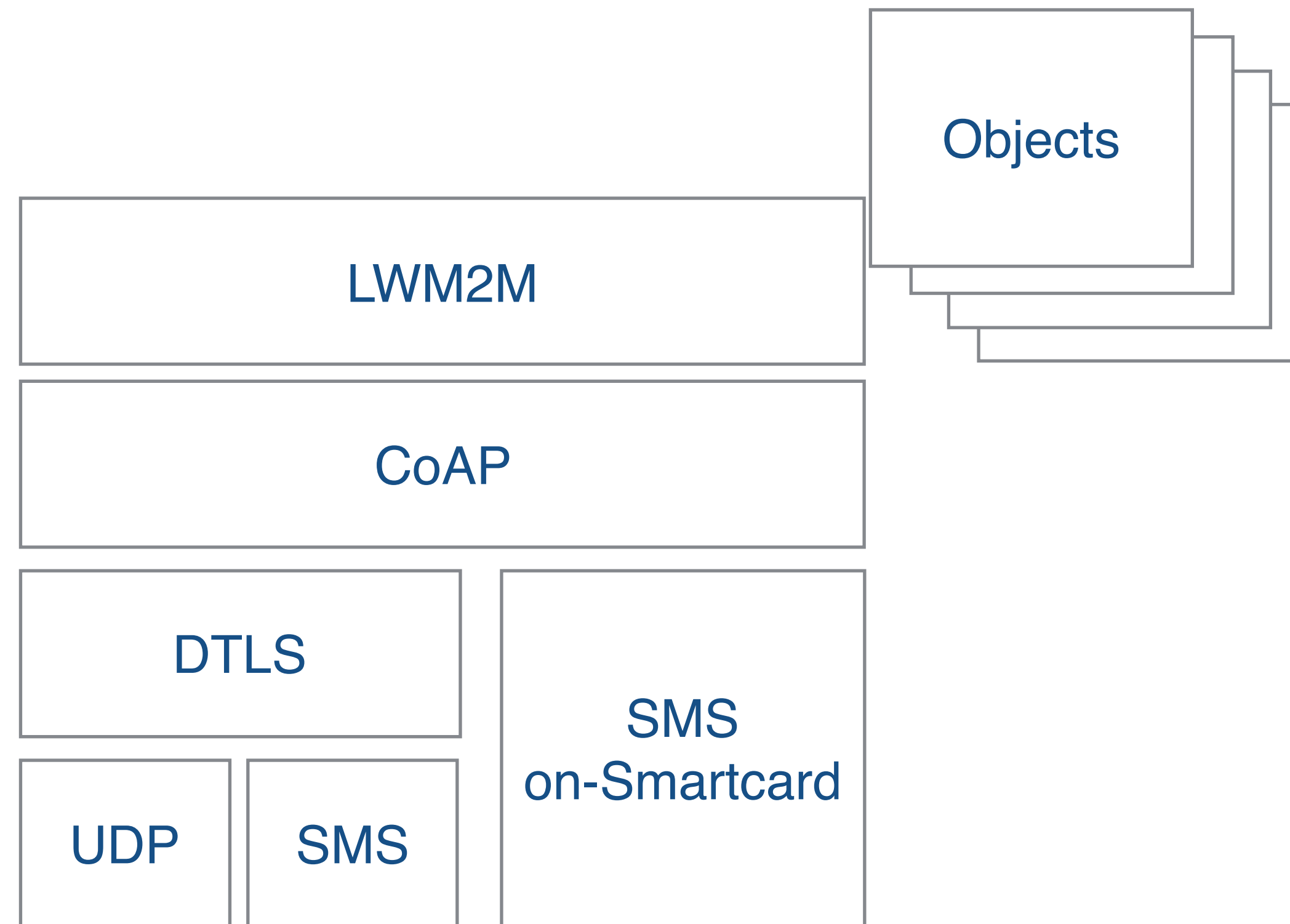
 @jaim - jaimejim.github.io



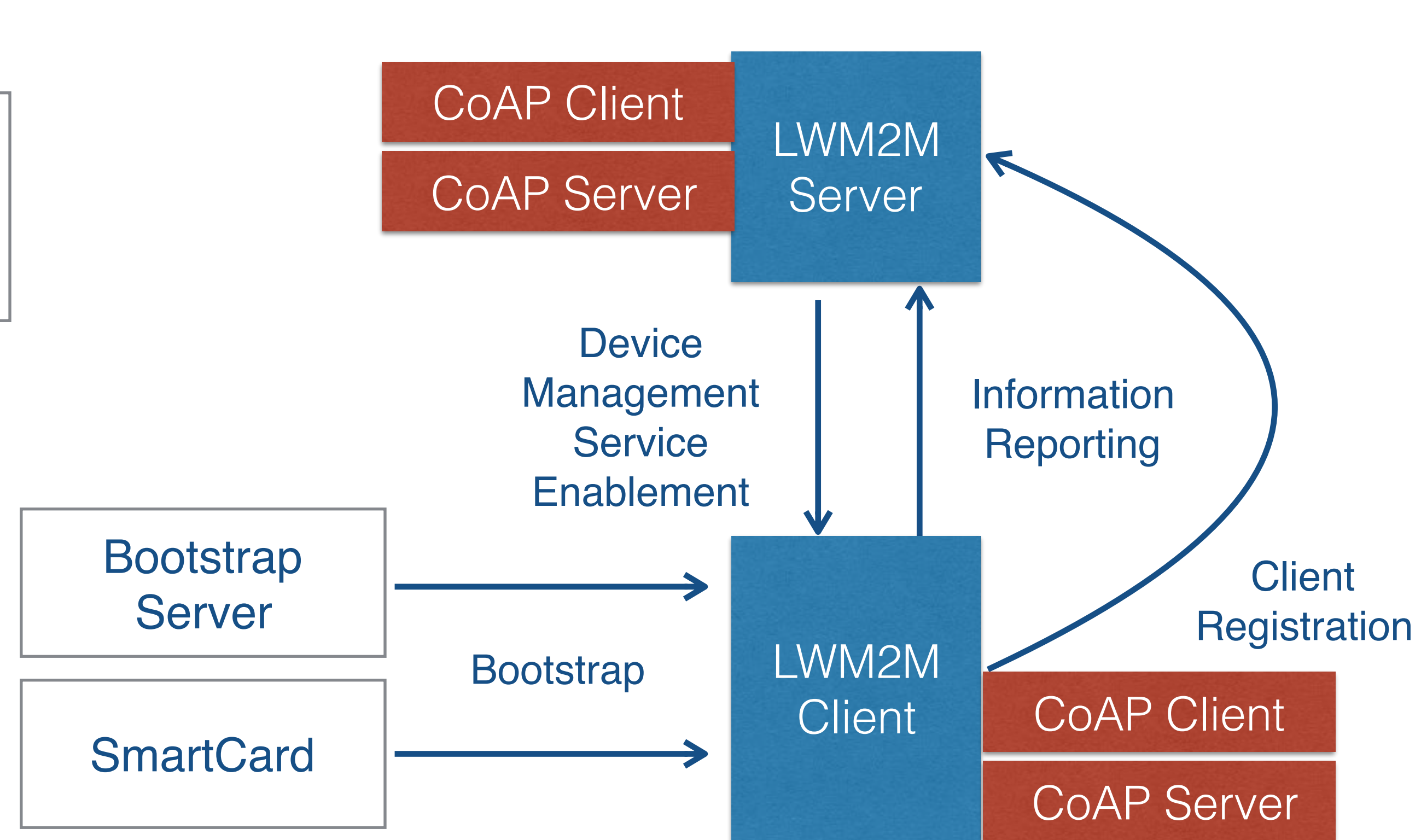
Problem Statement

- NATs and Firewalls are an issue for constrained devices.
- There does not seem to be one single solution to the problem.

Managed Devices with LWM2M



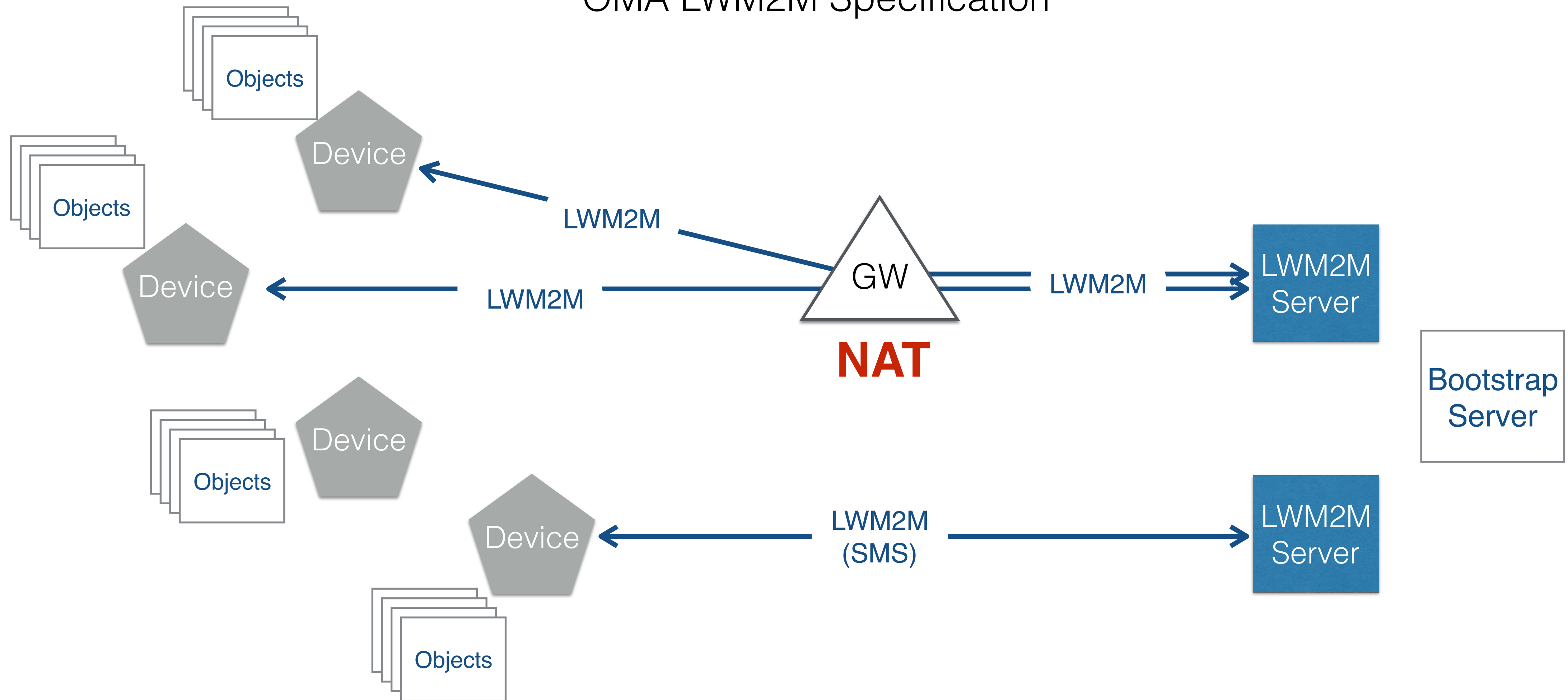
LWM2M Device Stack



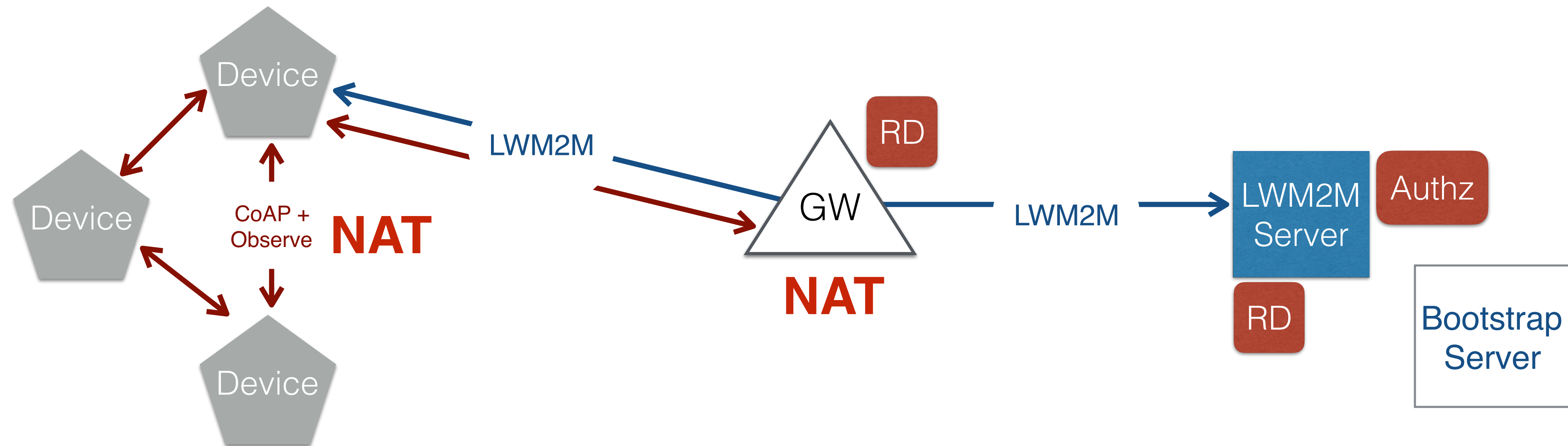
LWM2M Architecture

LWM2M Interactions

OMA LWM2M Specification



Interactions among CoAP EPs



Common solutions

1. Sending messages (either inside or outside of network) for punching holes in the NAT (PINGs, Keepalives...).
2. IPv6
3. Session Traversal Utilities for NAT (STUN), RFC5389
4. Socket Secure (SOCKS).
5. Traversal Using Relays around NAT (TURN) is a relay protocol designed specifically for NAT traversal.
6. Interactive Connectivity Establishment (ICE) and STUN.
7. UPnP Internet Gateway Device Protocol (IGDP).
8. NAT-PMP as an alternative to IGDP.
9. Port Control Protocol (PCP) as alternative to NAT-PMP, RFC6887.
10. Application-level gateway (ALG).

Common solutions

1. Sending messages (either inside or outside of network) for punching holes in the NAT (PINGs, Keepalives...).
2. IPsec *ideal*
3. Session Traversal Utilities for NAT (STUN), RFC5389
4. Socket Secure (SOCKS).
5. Traversal Using Relays around NAT (TURN) is a relay protocol designed specifically for NAT traversal.
6. Interactive Connectivity Establishment (ICE) and STUN.
7. UPnP Internet Gateway Device Protocol (IGDP). *updated*
8. NAT-PMP as an alternative to IGDP. *updated*
9. **Port Control Protocol (PCP) as alternative to NAT-PMP, RFC6887.**
10. Application-level gateway (ALG). *complex*

Basic Idea

Use standard PCP to signal the NAT.

+	-
Simple standard solution.	NAT configurations vary.
Added benefit of configuring firewalls too.	Firewall configurations too.
Low overhead and no keepalives.	Not much info on deployed NATs (to my knowledge)
No need for other transports than UDP.	
No need for other servers.	

General Operation in a managed CoAP endpoint

1. A CoAP device registers on RD or a management server.
2. If the binding is UDP then the device can enter in “PCP mode”.
3. The device should know the lifetime of the registration to a manager and/or the preferred length of the UDP session.
4. The device can send a PCP request to the default gateway (the one that provided the DHCP6 resolution) on port 5351 or on port 66 (CISCO).
5. If no response is received the device then tries the default Anycast address 2001:1::1/128 and awaits a response.
6. If no response then operate normally, PCP is not enabled. If response then PCP is enabled, longer UDP bindings have been set.

Deployment

Cisco

https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-3/cg_nat/configuration/guide/cgnat_cg43crs/cgc43cgn.html#39351

Requires Cisco running IOS-XR.

Juniper

https://www.juniper.net/documentation/en_US/junos/topics/example/nat-pcp-napt44.html

Requires Juniper MX with MS-DPC.

A10

https://nettools.net.berkeley.edu/tools/docs/a10/thunder/ACOS_4_1_0/html/v6_guide-Responsive%20HTML5/v6_guide/v6_pcp/v6_pcp.htm

An unorthodox link as it's not directly from A10, but their manuals are not public

F5

https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/cgn-implementations-11-5-0.html
https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/cgn-implementations-11-5-0/5.html#conceptid

To be done

- Find out current deployment on home gateways (NETGEAR and the like).
- Test!!!
- Work out first draft (WIP), LWIG, CORE.
- Beyond basic cases.
 - How to forward config to other NATs in between.
 - How to delegate to other endpoints.
 - Use of extra PCP features like MAP and PEER Opcodes.
 - Measurements of complexity and traffic.